⑲ 日本国特許庁 (JP)　　⑪ 特許出願公開

⑫ 公開特許公報 (A)　　昭57—55468

⑤Int. Cl.³	識別記号	庁内整理番号	⑬公開　昭和57年(1982)4月2日
G 06 F 15/00	102	6974—5B	
15/30		7737—5B	

発明の数　1
審査請求　未請求

(全 7 頁)

⑤④個人識別方式

⑳特　　願　昭55—129321
㉒出　　願　昭55(1980)9月19日
㉑発 明 者　藤方健二
国分寺市東恋ケ窪1丁目280番地株式会社日立製作所中央研究所内
㉑出 願 人　株式会社日立製作所
東京都千代田区丸の内1丁目5番1号
㉔代 理 人　弁理士　薄田利幸

明　細　書

発明の名称　個人識別方式

特許請求の範囲

1. 暗号化された個人データを2つに分割して共通の記憶手段および個別の記憶手段に記憶しておき、識別に際して、これらの手段からのデータを合成して解読し、解読された個人データをもとに質問を提示し、その質問に対する回答の正否を検定するようにしたことを特徴とする個人識別方式。
2. 特許請求の範囲第1項記載の個人識別方式において、個人データが個人の過去の経歴や経験に基づく知識情報であることを特徴とする個人識別方式。
3. 特許請求の範囲第1項または第2項記載の個人識別方式において、質問に対する回答を音声で入力し、かつ回答の正否を検定するとともに声の質の合否を検定するようにしたことを特徴とする個人識別方式。

発明の詳細な説明

本発明は、計算機システムが個人に対してサービスを提供する場合などにおいて、その個人があらかじめ登録された特定の個人であるかどうかを識別する方式に関するものである。

従来、個人識別では、個人の生理的・形態的特徴である顔とか指紋とか掌形とかサインとかを利用する方法や、個人の持物である印鑑とか磁気カードを利用する方法や、個人の記憶した番号(パスワード)を利用する方法が広く考察され、一部実用されている。

このうちのいくつかは、画像処理装置を必要とし、また、処理に多くの時間が掛かるなどから、実時間での識別に困難があるなど、問題が多い。また他のいくつかは、紛失・盗難など安全(セキュリティ)上の問題があり、これが用途を限定している最大の要因の一つとなつている。

したがつて本発明の目的は、画像処理装置のような特殊で高価な装置を必要とせず、かつ利用する個人にとつて極めて安全な個人識別方式を提供することにある。

上記の目的を達成するために、本発明の個人識別方式では、顔や掌形などのような外見的な特徴ではなく、もつと心の奥底にひそむもの、すなわち個人の過去の経歴や経験に基づいた「知識」を利用する。この知識データは一たん暗号化され、その暗号化されたデータが二分されて、一部は計算機システムに記憶され、残りの一部は個人の持物の中に記憶されるように構成する。この個人の持物とは、磁気カードであつてもよいが、より効果的には、電子回路を含む小型のカード状装置である。この装置は、従来の磁気カードがパッシブな記憶媒体でかつ記憶容量が比較的小さいのに対し、電子カードとも呼ぶべきアクティブ要素を持つた比較的記憶容量の大きい記憶媒体である。このように暗号化したあと二分して別々に記憶すると、この電子カード単体だけが盗難にあつても、あるいは逆に計算機システム内の個人の知識データが盗難にあつても、それぞれは不完全なデータであるため解読は不可能となる。したがつてこの二つのデータが合成され、かつ適切な鍵で解読され、かつ解読された知識データをもとに計算機システムが問合わせてくる質問にすべて正確に答えられたときだけが本人と識別されるので、極めて安全なシステムとなる。とくに本方式を銀行システムに応用する場合には、上述の電子カードは、単に個人識別用の知識データの記憶という機能だけでなく、金額データの管理の機能を付与した電子財布として用いることができ、従つて銀行の口座から個人識別が合格となつたときに預金をデータの形でこの電子カードにおろし、この電子カードで買物ができるようなシステムを構築することができる。

以下、本発明を実施例によつて詳細に説明する。

第1図は、本発明による個人識別方式が実装されるシステムの一例を示している。図において、ホスト計算機1のファイル装置2の中に、暗号化された個人の知識データの一部が格納されている。ホスト計算機1に接続された端末装置3の前に坐つた利用者は、自分の電子カード4を電子カード読取器5にセットし、キーボード6から自分のパスワードを入力する。電子カード4には少くとも2種類の情報が記憶されており、その第1種は既述の知識データの残りであり、第2種はファイル装置2の中から該当する知識データを探索するための情報である。第2種情報としてはたとえばファイル番号とか電子カードの発行番号が利用できる。この情報は個人のパスワードを鍵として暗号化されているので、キーボード6から入力されたパスワードで電子カード4から読取られた第2種情報を解読することによつて、ホスト計算機1がファイル装置2から対応した知識データの一部を取出すことができる。

取出された知識データは、電子カードに記憶された知識データとたとえば端末装置3で合成される。端末装置3は、それ自身で演算能力を持つインテリジエント端末とすることができる。合成された知識データをもとに、端末装置はそれを入力されたパスワードで解読し、その結果をもとに表示装置7の上に質問文を表示し、その回答の入力をうながす。この場合、付属されたスピーカ8により合成音声で質問を発してもよい。回答はキーボード6のキーによる入力が、あるいは付属されたマイクロホン9に向かつて音声で入力する。この場合、質問が「はい」「いいえ」で答えられるような形式とか、あるいは項目選択形式で1～5程度の数値のうちの1つを発声させて認識させる技術は既に実用の段階に十分達している。

第2図は、本発明の個人識別方式に用いられる電子カード4の具体的一実施例を示すブロック線図である。電子回路は近年の半導体技術の発展で極めて小型化・薄形化して実現可能であり、本実施例でも全体の大きさが通常のクレジットカードの大きさで、厚さも厚くてもその数倍以下で実現できる。この電子カードの中心部はマイクロコンピュータ11と電気的に書換え可能なROM12(EEPROM, electrically erasable and programable read-only memory)である。この実施例では、回路駆動用電源とROM書込用電源とが外部すなわち既述の電子カード読取器5から端子16，17を介して供給され、またそこと

の信号の授受は送受信制御回路１３と光変換素子１４の作用で、ビット直列の光信号として実行される。マイクロコンピュータ１１は、入力される複数個のコマンド信号に応じてそれぞれあらかじめ定まつたプログラムを実行する機能をもつており、その各プログラムはＲＯＭ１２の中に記憶されている。ＲＯＭ１２の一部には既述の第１種ならびに第２種の情報が入つており、この部分はマイクロコンピュータ１１の制御のもとに電源スイッチ回路１５を作動させて、必要なときに通常状態のときとは一般に異なつた書込用電源を供給するようにし、内容を書換えることができる。

第３図は本個人識別装置に用いる知識データの一例の一部を示す。ここで記号や数値はＡＳＣＩＩコードとして各１バイトで構成され、また漢字・かな類はＪＩＳ Ｃ６２２６に規定されたコードが利用でき各２バイトで構成できる。従つて第３図の情報は、とりもなおさず一連のバイトから構成された情報である。この情報は、個人の氏名，生年月日，性別，住所などの基本データの他、過去の経験や経歴に関した情報として、郷里を流れている小川の名前，登山したことのある思い出の山の名前，過去に住んだことのある都市，学生時代の恩師の名，愛用している腕時計のメーカ名，自家用車の登録番号，母の結婚前の姓などが、対応する項目番号のあとに列記されている。このうち都道府県名などは文字コードではなく、１が北海道、２が青森というようなコード番号として記憶してもよい。

このような知識データを用いて端末装置３が質問を発する技術は極めて容易に実現できる。たとえばもつとも簡単な方式としては、「あなたが」「は」「ですか？」という３種の文字コード列を記憶しておき、いくつかの項目のうちの一つ、たとえば第３図の（２８）塩釜市が乱数を利用して選ばれたとすると、端末装置は（２８）に対応してシステムが記憶している「過去に住んだことのある都市」という文字コードを質問の文字コードに挿入し、かつ回答の「塩釜市」という文字コードを挿入して、「あなたが過去に住んだことのある都市は、塩釜市ですか？」という文章を作り、これを表示装置７に表示すればよい。表示装置７は通常、漢字，かなどの文字発生器を内蔵し、表示バッファメモリに文字コードを書込むだけで表示が自動的に行なわれるよう簡単に構成できる。この時「はいか，いいえで答えて下さい」というふうに回答の仕方を表示して教示することもできる。また上例で塩釜市以外の市名を入れて「いいえ」の回答を期待することもできるし、さらに「あなたが」「は」「次のうちのどれですか？」という文字コード列を基本にして「あなたが過去に住んだことのある都市は，次のうちのどれですか？」という文章を創成し、１…米沢市　２…塩釜市　３…姫路市　４…境港市　５…松山市　というように５個程度を例示し、その中に本物の回答例「塩釜市」を任意の場所にはめ込んだり、あるいは全然はめ込まなかつたりして質問を複雑化できる。このような質問技術はすでに実際的な技術になつてきている。

第４図は、第３図のような個人の知識データを格納する方法を示した図である。知識データはそのままの形で（通常の文字コードとして）記憶すると、容易に判読でき、データの安全上の大きな問題がある。本個人識別方式ではこれを暗号化し、しかも暗号化した結果を２分して別々に記憶することを特徴とする。一般に暗号化のやり方は、ある鍵となる記号で、データをある一かたまり（以後、ブロックと呼ぶ）ずつ変換するものであり、米国商務省標準局が推奨するDES（Data Encryption Standard）と呼ばれる暗号化方式が利用できる。（注）：(Data Encryption Standard, 発行番号FIPS PUB 46, National Bureau of Standard, U.S. Department of Commerce) この方式では、第４図に示すように、原情報を８バイトずつに区切り、これを一かたまり（ブロック）として暗号化する。この時の鍵としては本人しか知らない８バイトのパスワードが使用できる。この暗号化方式は、８バイトのデータを６４ビットの一連の情報とみなし、まずビット位置をある所定の方法でばらばらに入れかえる

ことから始まる。次いで鍵で修飾された複雑な演算を数段回実行する。従つて出力から鍵なしでもとのデータを類推することは不可能であり、解読する唯一の方法は鍵を次々と片つ端からためしていくことである。ＤＥＳでは鍵として８バイトとつており、チエックビットを除いた５６ビットが自由にとれるので2^{56}通りの鍵が実在する。従つてこれを順次ためしていつて正しい鍵を見い出す平均時間は、ある計算(1μsに１個ずつ解読すると仮定）によれば１０００年となる。しかし問題は、実用的なシステムではこの鍵として2^{56}種もとれないことである。上述の例では、個人の入力するパスワードを鍵として暗号化するのが便利であるが、５６個の１，０のシーケンスをパスワードとして覚えるのは困難である。したがつて通常のテンキーのような数字キーボードから入力される番号をパスワードとする以外になく、その場合には従つて、８桁の数値としても10^8個の組合せしかない。これは上述と同じ計算では３分である。すなわち強力が計算機で解読すれば３分で内容が見えてしまう。このように、計算機どおしの暗号通信には強力な暗号化方式も、計算機と人間との接点で意外と弱さを露呈する。この弱さを確実になくするために、本発明の個人識別方式では、知識データをあるかたまりずつ暗号化したのち、各かたまりからその一部を抜出してしまうようにした。この方式では、データの安全性はその抜出した量、残つている量のどちらか小さい方に依存している。すなわち５個のかたまりから各１ビットずつ抽出すれば、残つたデータでこの計５ビットを推測するには2^5通りためせばよい（実際にはそれをさらに10^8個の鍵でためすことになる）。もし５個のかたまりから１バイトずつ抽出すれば、残つたデータでこの計５バイトを推測するには2^{40}通りの試みが必要となる。従つて抽出するデータと残つているデータがいずれもが最高の安全性を保つのは、理論的には丁度半分ずつに分ける時である。上の例では、原情報８バイトを同じく８バイトの暗号化情報へと変換したあと、４バイトずつに変換し、図示したように一方をホスト計算機１の持つファイル装置２の中に記憶し、他方を個人が所有する電子カード４の中のＲＯＭ１２の中に個人ファイルとして記憶するように構成する。

このようにすると、上例の５つのかたまり（ブロック）からなる情報（すなわち４０バイト）は２０バイトずつに分離され、どちらか一方で他方を鍵なしで推測するとすれば、鍵を８桁の数値（すなわち10^8通り）として、

$$2^{32\cdot5}\times10^8$$

通りの回数の試算が必要となり、これは実際上解読が不可能な値である。しかもその試算のうちの何度かに、もつともらしい情報が出現するのでさらに解読を困難とする。たとえば第３図の例でいえば、第４図の第１ブロックに相当する情報は「（０１）磯野」である。「（０１）」は各１バイト、「磯野」は各２バイト、計８バイトの情報であるからである。このとき解読の過程で「磯田」「磯口」「磯島」「上野」「山野」など、もつともらしい多様な解読結果が出現することになる。(01)(02)(03)というふうに数字が順番に入つているということがわかればまた解読は多少楽になるが、もともとデータが半分欠除しているわけだからそう極端に楽になるわけではない。

以上のように、暗号化したデータを各暗号化の単位ごとに２分して別々に記憶するようにすると、その安全性は極めて大きくなる。この場合、原情報量が多ければ、必ずしも１／２ずつに分離する必要はない。すなわち各ブロックから少しずつ抽出しても、ブロック数が多ければそれだけ組合せの数は大きくなり、従つて必要な安全性を保つのに十分なだけのデータの抽出で済む。この方式では、既述のごとく両方が組合されて、かつ正しい鍵が提示されたときのみ解読ができることになる。

第５図は、本発明の個人識別方式のための知識データを作る装置の一実施例を示している。ホスト計算機１に接続されたデータ作成用端末装置３３には、ホスト計算機１から提示される質問を表示するための表示装置７と、その回答を入力するためのデータ入力回路３６と、その入力された

データがあるバイト数になるまで保持するデータ保持回路３７とをもつている。入力データが一定バイト数（すなわち１ブロック）に達するたびに、別途入力されて鍵レジスタ３８に保持された鍵番号で、これを暗号化する暗号化回路３９を作動させ、得られた暗号出力を分割回路４０で二分して一方をホスト計算機１経由でファイル装置２に送り出し、他方を電子カード書込み装置４４で電子カード４に書込むように構成される。この場合、データ入力回路３６は原理的には漢字タブレットのような多文字入力キーボードでよいが、マンマシン性の向上のためには、表示装置に表示する質問をできるだけ選択方式にすれば、簡単な英数字キーでも実現できる。

以上に述べた個人識別方式は、たとえば銀行システムに応用することができる。すなわち既に示した第１図において、ホスト計算機１は銀行の計算機として金銭出納の管理をも行なつているとする。このとき、窓口の端末装置３にむかつて利用者が自分の電子カード４を電子カード読取り器５にセットし、表示装置７に表示される質問に次々と回答する。本人であることが確認されたとき、端末装置３は、電子カード４に入つている第３種の情報を読み出し、これを表示装置に表示する。この第３種の情報とは、既述の第１種，第２種に加えて記憶された預金額の情報である。したがつて利用者は自分の電子カードに入つている預金額を知ることができ、また、別途、自分の銀行口座に残存する預金額も同時に簡単に表示できるので、これらをみて、口座からどの位の額をおろして電子カードに入れるかを判断し、キーボード６からその額を入力する。端末装置は、電子カードに残存した預金額と入力された預金引出し額とを加算して、これを暗号化し、再び電子カード内に書込む。この電子カードは、いわば電子財布であつて、商店の金銭登録機と組合わせて、買物総額をここから自動的に引落とすことが容易にでき、キャッシュレスの買物が可能となる。

この個人識別方式では、第３図の項目（１００）に例示したように、個人の音声の特徴データを含めることができる。この特徴データは、ある言葉を発声したときの音声分析によつて得られるデータであり、たとえばPARCOR 係数であつてよいし、さらに他の音質特徴を付属させてもよい。このようにするとき、個人識別の一質問として項目（１００）が選ばれると、端末装置は「合言葉を入力下さい」というように指示する。利用者はあらかじめ登録した合言葉を喋ると、それが分析されて、項目（１００）に記憶されたものと、内容的に一致するかどうかとともに音声的に一致するかどうかも調べることができる。このような声質的な一致をみるには、いくつかの質問項目のうちのただ一つ（すなわち項目（１００））に限る必要はない。どの質問に対しても音声で回答を入力するようにすれば、「はい」「いいえ」「３番」などというような短い言葉の中からも、その人の声質を分析すれば、かなり正確な判断が可能となる。このように、電子カードの中に声の特徴データを含めることができるので、回答内容の正否とともに声質の合否をも検定することが可能となり、したがつて銀行システムに実用するとき、利用者は銀行の計算機システムと対話するために窓口に行く必要はなく、任意の電話器で預金を電子カードにおろすことが可能となる。この場合、質問は、すでに成熟期にある音声合成技術によつて容易に実現できるし、その回答音声の認識も容易になつてきている。また電子カードはアクティブな回路要素を含むので、第２図で述べた構成のうち光変換素子１４を音変換素子と置換すれば、従来の音響カップラによつて容易に通信が可能となり、送られてくるコマンドによつて電子カードの内容を送り出したり書換えたりが自由にできる。

以上説明したごとく、本発明によれば、安全な個人識別方式が実現でき、銀行システムを初めとして各種のサービスシステム、予約システム、セキュリティシステムなどに実用でき、その効果は極めて大である。

図面の簡単な説明

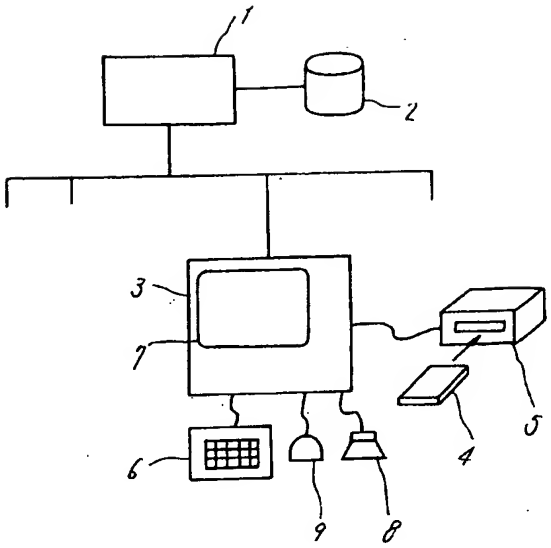
第１図は、本発明による個人識別方式が実装されるシステムの一例を示す図、第２図は本発明の

個人識別方式に用いられる電子カードの一具体的実施例を示すブロック線図、第３図は、本発明の個人識別方式に用いる知識データの一例を示す図、第４図は第３図に示したような知識データを格納する方法を示した図、第５図は本発明の個人識別方式のための知識データを作る装置の一実施例を示す図である。

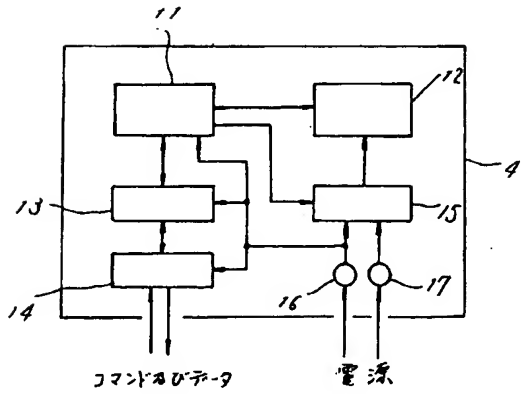
１…ホスト計算機、２…ファイル装置、３…端末装置、４…電子カード、５…電子カード読取器、６…キーボード、７…表示装置、８…スピーカ、９…マイクロホン、１１…マイクロコンピュータ、１２…電気的書換え可能メモリ（EEPROM）、１３…送受信制御回路、１４…光変換素子（または音変換素子）、１５…電源スイッチ回路、３３…データ作成用端末装置、３６…データ入力回路、３８…鍵レジスタ、３９…暗号化回路、４０…分割回路、４４…電子カード書込み装置。

代理人　弁理士　薄田利幸

第　１　図



第　２　図

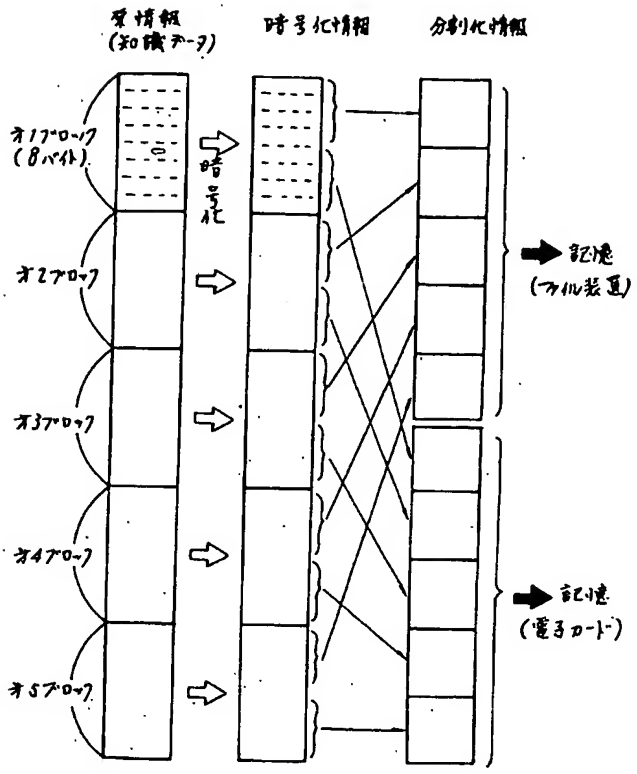


第　３　図

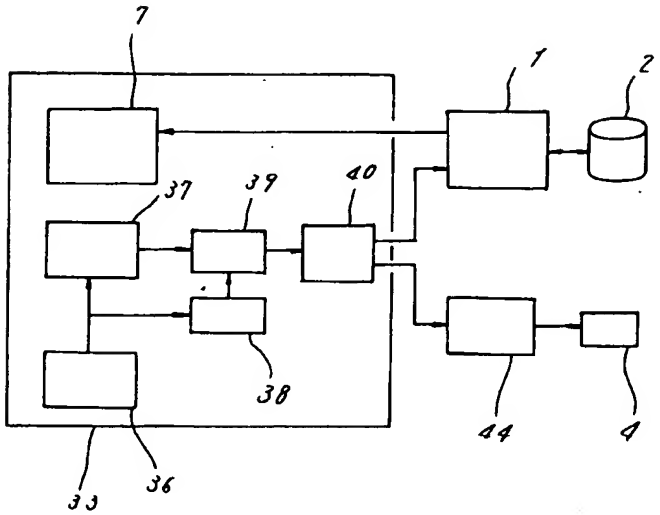
(01) 磯野サザエ (02) 昭和35年4月1日 (03) 女
(04) 東京都 (05) 国分寺市
---
(26) 日野川 (27) 越智山 (28) 塩釜市 (29) 新田
しずき (30) セイコー (31) ﾌﾈ摩 55-1234 (32) 長谷川

---
(100) 10, 8, 3, 5, 9, 138, 26, 10, 9, 3, 281, 6

第 4 図


原情報
(知識データ)
暗号化情報
分割化情報
ブロック
(8バイト)
暗号化
記憶
(ファイル装置)
記憶
(磁気カード)

第 5 図


7
1
2
37
39
40
38
44
4
33
36